



2.48. PRIVACY POLICY & GENERAL DATA PROTECTION REGULATIONS

2.48.1. PRIVACY POLICY - INTRODUCTION

We at Sherpa know that you care how information about you is used and shared and we appreciate your trust in us to do that carefully and sensibly. This Privacy Policy (“Policy”) is meant to help you understand what personal information we collect, why we collect it and what we do with it. This includes how long personal information is retained for and how we ensure it remains secure. It also sets out your individual rights over your personal information, and how to contact us with any queries.

If we make changes we consider to be important or if we plan to use personal information for a new purpose, we will let you know by updating the Policy on our website and/or contacting you using other methods such as email. Your privacy matters to us so whether you are a new or existing client or a member of staff.

Please do take the time to get to know our practices – and if you have any questions about our privacy practices or your personal information choices please contact us at GDPR@ays.co.uk.

2.48.2. CONTROLLERS OF PERSONAL INFORMATION

Any personal information provided to or gathered by us is controlled by Sherpa Ltd.

As controllers of personal information, we are responsible for the accuracy and security of this information. We will only collect the information we require and are lawfully permitted to collect, and we will use this information in the ways which you would reasonably expect us to.

2.48.3. THE INFORMATION WE COLLECT AND HOW WE USE IT

We collect personal information to aid us in delivering and continually improving the quality of our staffing service, as well as fulfilling contractual commitments to both our clients and our members of staff.

When you interact with us, we may ask you for the following information:

- personal and contact details (for example your name, email address, contact number);
- personal and contact details you give us when subscribing to receive emails, newsletters or marketing information from us;
- To enable our systems to recognise your device and to provide features to you when you visit us online, we use cookies. For more information about cookies and how we use them, please read our Cookie Policy at http://www.eventsherpa.co.uk/Cookies_Policy.pdf;
- your IP address;
- information you provide if you report a problem with our website or service.

Additionally, for members of staff:

- during pre-assignment vetting we will request details from you including, your name, your work history, qualifications, contact details (such as email, telephone number and home address), gender, your right to work documents, details required for equality and discrimination legislation checks and your personal preferences, choices and requirements specific to particular requests or services;



- details of your education, employment history, bank details and national insurance number, references, right to work and other information you tell us about yourself (e.g. the information contained within your CV) when you engage with us for the provision of services;
- information from social media activity (such as likes, shares and tweets) when you interact with us on social media;
- additional information which you provide voluntarily and/or which we may ask from you to better understand you and your interests;
- We may also collect sensitive Personal Information about you (including details of your physical or mental health, racial or ethnic origin, criminal allegations or offences, trade union membership and/or other sensitive Personal Information that you may choose to provide to us voluntarily from time to time.

We do not undertake automated decision making or profiling using your data, and we will notify you if this position changes.

2.48.4. WHY DO WE COLLECT YOUR PERSONAL INFORMATION?

We collect and use your personal information because it is necessary to obtain certain details which includes personal information from you in the work-searching process and it is in our legitimate interests in the course of operating our business, including:

- responding to your queries;
- providing work-finding services and/or information to you;
- transmitting Personal Information between our offices or functions for internal administrative purposes;
- setting you up on a work assignment with a client; and/or
- carrying out direct marketing.

We will only collect, use and handle your Personal Information when:

- it is necessary for our legitimate interests in connection with carrying out our business, as long as, in each case, these interests are in line with applicable law and your legal rights;
- and/or where you have agreed;
- and/or where this is necessary for legal obligations which apply to us.

2.48.5. HOW WE USE THE INFORMATION YOU GIVE US

As a prospective or existing client, we might ask you to provide contact details (for example your name, email address, postal address and telephone number) which we use to establish a relationship with you and provide information about our services.

Additionally, for a member of staff, we undertake the following processing of your personal information on the legal basis that it is necessary to perform our contract with you and to provide the services we have agreed to provide to you. Where we have not entered into a contract with you, we may also carry out this processing because in that pre-contractual stage where we consider it is necessary in our legitimate business interests in order to deal with requests, enquiries or comments you have made to us.

- Submission of details to clients – if you register to apply for a particular role, request to be put forward for a role or if you have asked us to put you forward for suitable roles, we will share some of your personal details including your name, work history and qualifications with our clients offering potential roles which might be suitable for you.



- On-boarding for a work-assignment – If you are offered and accept a work assignment through us, we will need further personal information from you such as NI number, bank details, emergency contact details and some medical information in order to fulfil our statutory and contractual obligations to both you and our client.
- Reporting to clients and managing timesheets, payroll and work performance – We sometimes have to prepare reports for clients relating to the services provided by us for example reports on financial or administrative matters or compliance with legal requirements. Such reports may contain your personal information such as your name, hours worked and pay rate.
- Other lawfully permitted processing – We may also use any personal information that you provide to us for example to other affiliated companies or to any other company who you ask us to approach on your behalf for work-searching purposes. If you choose not to provide personal information requested by us, we may not be able to provide you with the services and/or information you have requested or otherwise fulfil the purpose(s) for which we have asked for the personal information, including placing you in a work-assignment. We will where possible anonymise or aggregate such data for reporting purposes.
- We undertake Pre-Assignment vetting – we collect your personal information which you provide to us when applying for a role or registering for our job-finding services to comply with our (and clients’) legal obligations regarding your right to work and any necessary qualifications for roles,. We may also process your personal information for this purpose where we consider it necessary for performance of the contract with you, or otherwise with your consent

We undertake the following processing of your personal information with your consent:

- Marketing – where legally permitted to do so where you have provided us with your contact details and have agreed to be contacted for marketing purposes, we may contact you by telephone or by post for marketing purposes relating to our services, our website, and/or to research opinion on proposed business developments. Your agreement to the use of your Personal Information for these purposes is optional (see Marketing Opt-out below) and if you fail to provide your agreement, your use of our work-finding services will not be affected.

2.48.6. INFORMATION FROM OTHER SOURCES.

To comply with our legal and regulatory requirements to perform background checks (including right to work), we use data provided by third party agencies.

2.48.7. SHARING YOUR DATA WITH THIRD PARTIES

Some services that we provide require the involvement of third parties. We have carefully selected these third parties and taken steps to ensure that your personal information is adequately protected. The third parties may include our clients, suppliers of IT services, third party time and attendance services or vetting services.

We may employ third party companies to process personal information provided by us on our behalf for business functions, including (without limitation) IT support, hosting our data on cloud platforms, legal, accounting, audit, consulting and other professional service providers, and providers of other services related to our business.

Portions of our services may be provided by organisations with which we have a contractual relationship, including subcontractors, and, accordingly, your Personal Information may be disclosed to them. We only provide these organisations with the information that they need to be able to perform their services.



We will have in place an agreement with our service providers which will restrict how they are able to process your Personal Information.

2.48.8. TRANSFERS OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (“EEA”)

Where your information is transferred outside the EEA to other countries in which applicable laws do not offer the same level of data privacy protection, your rights and protections remain with your data. We put measures in place to ensure that all transfers are managed lawfully.

2.48.9. SHARING WITH OTHER THIRD PARTIES

We may also provide your information to other third parties such as regulators and law enforcement agencies, where we are required by law to do so, where necessary for the purposes of preventing and detecting fraud, other criminal offences and/or to ensure network and information security.

2.48.10. HOW LONG DO WE KEEP YOUR DATA FOR?

It is our objective to retain your personal information for the length of time required for the specific purpose or purposes for which it was collected, which are set out in this policy. However, on occasion we may be obliged to store some data for a longer time, for example, where a longer time period is required by applicable laws. In this case, we will ensure that your Personal Data will continue to be treated in accordance with this policy.

2.48.11. HOW SECURE IS YOUR PERSONAL INFORMATION?

We employ appropriate security measures to help protect your personal information and guard against access by unauthorised persons. Information storage is on secure computers in a secure environment, or in secure, locked storage in the case of hard copy information. The information is encrypted wherever possible and we undergo periodic reviews of our security policies and procedures to ensure that our systems is secure and protected. However, the transmission of information via the Internet is not completely secure so we cannot guarantee the security of your information when it is transmitted to our website or from third party websites.

We acknowledge that the information you provide may be confidential. We do not sell, rent, distribute or otherwise make personal information commercially available to any third party, but we may share information with our service providers for the purposes set out in this Privacy Policy. We will keep your information confidential and protect it in accordance with our Privacy Policy and all applicable laws.

2.48.12. WHAT ARE MY PERSONAL INFORMATION CHOICES?

You can always request access to the personal information we hold about you and we will provide this to you subject to any regulatory requirements or exemptions. Before providing data to you, we will ask you for proof of identity and sufficient information about your interaction with us so that we can locate any relevant data for you.

- You may request access to or copies of the personal information that we hold about you by emailing us at GDPR@ays.co.uk or contacting your investment manager.



- If you believe that any of the personal information we have about you is incorrect or incomplete, please contact us as soon as possible. We will take steps to seek to correct or update the information.
- You may request that your personal information be deleted however this may not always be possible due to legal requirements and other obligations.
- Where we are processing your personal information for the purposes of performing our contract with you, you have the right to request that the personal information we hold about you be transferred to a third-party data controller.
- You may withdraw your consent to receiving marketing information at any time by emailing us at GDPR@ays.co.uk.

If you are unhappy with the way that we have handled your personal information, you can raise your concern to the Information Commissioners Office (ICO) in the UK (casework@ico.org.uk). Or alternatively please ask us for assistance.

2.48.13. CONTACT US

If you have any questions in relation to this Privacy Policy, or if you would like to contact us to exercise your rights as stated in this Privacy Policy, please contact GDPR@ays.co.uk.

2.48.14. GENERAL DATA PROTECTION REGULATIONS

The Company complies with the European Union's General Data Protection Regulations (GDPR) 2018 (Regulation (EU) 2016/679). For further information on the act please refer to:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>

This Policy will be regularly reviewed as the General Data Protection Regulation legislation is implemented.

We are committed to:

- ensuring that we comply with the six data protection principles, as listed below
- meeting our legal obligations as laid down by the European Union's General Data Protection Regulation (GDPR) 2018 (Regulation (EU) 2016/679)
- ensuring that data is collected and used fairly and lawfully
- processing personal data only in order to meet our operational needs or fulfill legal requirements
- taking steps to ensure that personal data is up to date and accurate
- establishing appropriate retention periods for personal data
- ensuring that data subjects' rights can be appropriately exercised
- providing adequate security measures to protect personal data
- ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues



- ensuring that all staff are made aware of good practice in data protection
- providing adequate training for all staff responsible for personal data
- ensuring that everyone handling personal data knows where to find further guidance
- ensuring that queries about data protection, internal and external to the organisation, is dealt with effectively and promptly
- regularly reviewing data protection procedures and guidelines within the organisation.

The General Data Protection Regulation (GDPR) 2018 (Regulation (EU) 2016/679) applies to the processing of personal data. The Authorisation to Work Procedure and application of the Baseline Personnel Security Standard involves processing of such data and Sherpa Ltd ensures that data is:

- 1) "processed lawfully, fairly and in a transparent manner in relation to individuals;
- 2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- 3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- 5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- 6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Sherpa Ltd is entered in the register as a Data Controller with the Information Commissioners Office.

Staff may only work for the company provided they have been authorised to work. Please refer to our Authorisation to Work Procedure.

We understand that an individual's refusal to undergo an essential check where there are no alternatives could lead to refusal of employment and that this is consistent with the General Data Protection Regulation (GDPR) 2018.

In such cases individuals will be made aware that it will not be possible for them to be Authorised to Work should they refuse. This is distinct from making a particular check of a condition of employment



where it may not actually be necessary. All checks will be carried out uniformly on a non-discriminatory basis and privacy rights, where relevant, will be respected.

Decisions whether or not to employ an individual are not based solely on the terms of our adoption of BPSS. Sherpa has undertaken to make employees and prospective employees aware of requirement for BPSS checks in its job advertisements and in its employee information literature.

Sherpa Ltd does not currently require its employees to have submitted a Basic Disclosure Certificate.

2.48.15. POLICY REVIEW RESPONSIBILITY

This policy is the responsibility of all staff employed within the Company. However, the updating of this document to ensure current legislation is complied with is the responsibility of the Board of Directors.

Further information can be obtained from the Office Manager.

DATE APPROVED: 22nd May 2018
POLICY REVIEW DATE: 12th April 2019



2.49. REHABILITATION OF OFFENDERS POLICY

2.49.1. INTRODUCTION

PURPOSE

Sherpa Ltd is committed to the principle of equality of opportunity and, subject to the over-riding consideration of protecting children and vulnerable people, undertakes to treat all applicants for positions fairly and not discriminate unfairly against any subject of a Disclosure on the basis of conviction or other information revealed.

AUDIENCE

This policy applies to all potential job applicants. This policy has particular reference to those concerned with recruitment. Responsibility for the implementation, monitoring and development of this policy lies with the Recruitment Manager. Day to day operation of the policy is the responsibility of departmental chief officers who will nominate a representative to ensure that this policy is adhered to.

FRAMEWORK

As an organisation using the Disclosure and Barring Service (DBS) / Disclosure Scotland to assess applicants' suitability for positions of trust, Sherpa complies fully with the DBS Code of Practice.

Sherpa is committed to the fair treatment of its staff, potential staff or users of its services, regardless of gender, disability, race, colour, ethnic or national origin, nationality, sexuality, marital status, age, religious or political beliefs or offending background.

RECRUITMENT OF EX-OFFENDERS

This policy also relates to the Rehabilitation of Offenders Act 1974.

2.49.2. POLICY STATEMENT

This written policy on the recruitment of ex-offenders is made available to all Disclosure applicants at the outset of the recruitment process.

We actively promote equality of opportunity for all with the right mix of talent, skills and potential and welcome applications from a wide range of candidates. We select all candidates for interview based on their skills, qualifications and experience.

A Disclosure is only requested after a thorough analysis has indicated that one is both proportionate and relevant to the position concerned. For those positions where a Disclosure is required applicants will be informed that a Disclosure will be requested in the event of them being offered the position.

Where a Disclosure is to form part of the recruitment process, we encourage all applicants called for interview to provide details of their criminal record at an early stage in the application process. We request that this information is sent under confidential cover to a designated person within Sherpa and we guarantee that this information is only seen by those who need to see it as part of the recruitment process.

Unless the nature of the position allows Sherpa to ask questions about your entire criminal record, we only ask about "unspent" convictions as defined in the Rehabilitation of Offenders Act 1974.



We ensure that all those in Sherpa who are involved in the recruitment process have been suitably trained to identify and assess the relevance and the circumstances of offences. We also ensure that they have received appropriate guidance and training in the relevant legislation relating to the employment of ex-offenders, eg the Rehabilitation of Offenders Act 1974.

At interview, or in a separate discussion, we ensure that an open and measured discussion takes place on the subject of any offences or other matter that might be relevant to the position. Failure to reveal information that is directly relevant to the position sought could lead to withdrawal of an offer of employment.

We make every subject of a DBS Disclosure aware of the existence of the DBS Code of Practice and make a copy available on request. We undertake to discuss any matter revealed in a Disclosure with the person seeking the position before withdrawing a conditional offer of employment.

Having a criminal record will not necessarily bar applicants from working with us. This will depend on the nature of the position and the circumstances and background of the offences with due consideration given to our responsibilities to protect children and vulnerable people.

- When “unspent” convictions have been disclosed we will consider:
- Whether the offence would cast doubt on the individual’s or the Company’s reputation
- Whether the offence would affect an individual’s ability to do the job
- Whether the conviction is relevant to the particular post
- The length of time since the offence occurred
- The nature and background of the offence (eg violent crime or a history of violence which may impact on our duty of care to our staff)
- The seriousness of the offence
- Whether there is a pattern of offences

We understand that certain types of employment and professions are exempt from the rules allowing applicants to reveal only unspent convictions and in those cases particularly where the employment is sought in relation to positions involving working with children or vulnerable adults, details for all criminal convictions must be given.

Complaints: any applicant wishing to raise a complaint should do so, in writing, to the Managing Director within 15 working days, at the latest, of the alleged incident. An investigation will then be conducted by a Director of the Company who has not been previously involved in the selection procedure. The Director’s ruling will be final. The individual will receive written notification as to the outcome.

2.49.3. POLICY REVIEW RESPONSIBILITY

This policy is the responsibility of all staff employed within the Company. However, the updating of this document to ensure current legislation is complied with is the responsibility of the Board of Directors.

Further information can be obtained from the Office Manager.

DATE APPROVED: 13th April 2018
POLICY REVIEW DATE: 12th April 2019